Elliptic Curves

Matthew McCarthy

Christopher Newport University

CNU Math Contest
November 2015

Algebraic Structures

"Definition" 1 (Set)

A *set* is a gathering of distinct numbers.

"Definition" 2 (Group)

A *group* is a set of numbers in which we can add and subtract any two numbers while remaining inside the set.

"Definition" 3 (Field)

A *field* is a set of numbers in which we can add, subtract, multiply, and divide any two numbers (excluding division by zero) while remaining inside the set.

Working Definition of an Elliptic Curve

"Definition" 4 (Elliptic Curve (from [?]))

An *elliptic curve* over a field $\mathbb{F}$ is a nonsingular cubic equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}$.

Definition 1

An equation of the form of Equation **??** is called a *Weierstrass equation*.

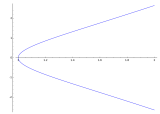

Figure: $y^2 = x^3 - 1$

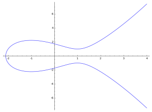

Figure:
$y^2 = x^3 - 3x + 3$

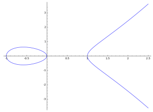

Figure: $y^2 = x^3 - x$

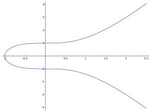

Figure: $y^2 = x^3 + 1$

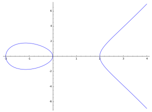

Figure: $y^2 = x^3 - 4x$

An elliptic curve over a field forms a group under the chord and tangent rule [?].

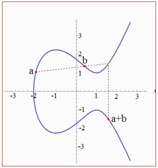

Figure: $a + b$

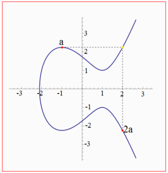

Figure: $2a$

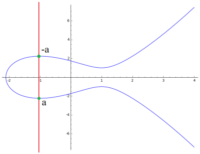

Figure: $a - a$

Where will the chord between a and $-a$ intersect the curve again?

Where will the chord between a and $-a$ intersect the curve again?

Where do parallel lines meet?

Where will the chord between a and $-a$ intersect the curve again?

Where do parallel lines meet?

At infinity!

Fermat's Last Theorem

Theorem 1

For $n \geq 3$, the equation

$$x^n + y^n = z^n$$

has no solutions when x,y, and z are natural numbers.

- This theorem was conjectured by Pierre de Fermat in 1637
- Proved by Andrew Wiles in 1994 using elliptic curves

Cryptography

- We call the set of remainders when dividing by a prime, $\mathbb{Z}_p$.
- The logarithm of a number, $\log y$ is a solution to the equation $e^x = y$.
- The discrete logarithm of a point on an elliptic curve is a solution to the equation $kP = Q$.
- On elliptic curves over $\mathbb{Z}_p$, finding the discrete log of a point is hard.

This means we can use it for cryptography!

References I

Steven D. Galbraith
Mathematics of Public Key Cryptography

Richard Schroeppel and Cheryl Beaver
Algorithms for Improved Performance in Cryptographic Protocols
Sandia National Laboratories. In: SAND REPORT (2003-4283)a

Joseph H. Silverman
The Arithmetic of Elliptic Curves
Graduate Texts in Mathematics

Avner Ash and Robert Gross
Elliptic Tales

Thank you!